U-Center2.0产品涉及漏洞Linux Polkit权限提升漏洞（CVE-2021-4034）

U-Center 2.0 汤祺 2022-01-30 发表

漏洞相关信息

漏洞编号： CVE-2021-4034

漏洞名称： Linux Polkit权限提升漏洞

产品型号及版本： PLAT_2.0_E0613P01及PLAT_2.0_E0706以前版本都涉及，具体可通过解决方案第二步查看polkit版本确认是否涉及

漏洞描述

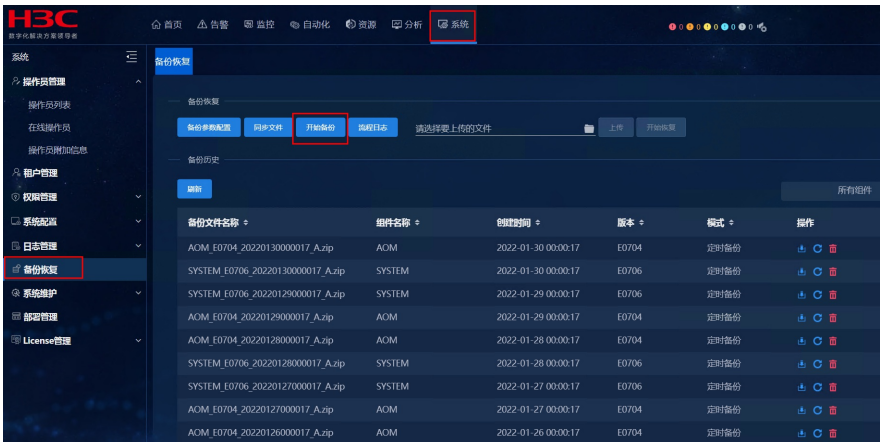
Polkit 默认安装在各个主要的 Linux 发行版本上，易受该漏洞影响的 pkexec 组件无法正确处理调用参数，并会尝试将环境变量作为命令执行。攻击者可以通过修改环境变量，从而诱导 pkexec 执行任意代码，利用成功可导致非特权用户获得管理员权限。

漏洞解决方案

漏洞解决方案

1、进行漏洞修复前，需先登录matrix页面进行数据备份，以及登录UCenter页面进行业务数据备份。

UCenter2.0数据备份：



matrix页面备份：

2、查看当前操作系统中Polkit版本是否涉及该漏洞，查看方法如下：

分别登录后台节点，通过命令查看：rpm -qa | grep polkit，查询当前系统的polkit的版本为polkit-0.112-18.el7_6.1.x86_64，需升级到新版本polkit-0.112-26.el7_9.1.x86_64

```
[root@matrix01 ~]# rpm -qa | grep polkit
polkit-pkla-compat-0.1-4.el7.x86_64
polkit-0.112-18.el7_6.1.x86_64
[root@matrix01 ~]#
```

3、下载最新版本polkit安装包，使用本案例附件解压后上传至节点后台，或者通过如下路径自行下载

下载路径：polkit-0.112-26.el7_9.1.x86_64.rpm版本在https://pkgs.org/search/?q=polkit网站获取的CentOS7->CentOS Updates x86_64目录下获取

4、将下载的安装包上传至集群所有后台节点中，进入对应目录，执行如下命令进行升级：

rpm -Uvh polkit-0.112-26.el7_9.1.x86_64.rpm

```
[root@matrix01 ~]# rpm -Uvh polkit-0.112-26.el7_9.1.x86_64.rpm
警告：polkit-0.112-26.el7_9.1.x86_64.rpm: 头V3 RSA/SHA256 Signature, 密钥 ID f4a80eb5: NOKEY
准备中...                          ################################# [100%]
正在升级/安装...
   1:polkit-0.112-26.el7_9.1          ################################# [ 50%]
正在清理/删除...
   2:polkit-0.112-18.el7_6.1          ################################# [100%]
[root@matrix01 ~]#
```

5、升级完成后，使用rpm –qa | grep polkit查询polkit升级新版本成功

```
[root@matrix01 ~]# rpm -qa | grep polkit
polkit-pkla-compat-0.1-4.el7.x86_64
polkit-0.112-26.el7_9.1.x86_64
[root@matrix01 ~]#
```

6、使用service polkit restart重启服务

```
[root@matrix01 ~]# service polkit restart
Redirecting to /bin/systemctl restart polkit.service
[root@matrix01 ~]#
```